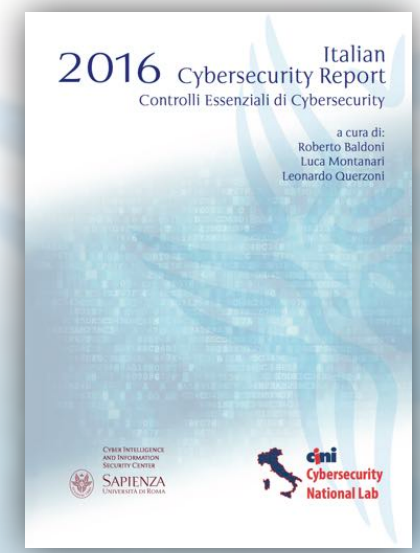
FRAMEWORK NAZIONALE PER LA CYBERSECURITY E CONTROLLI ESSENZIALI

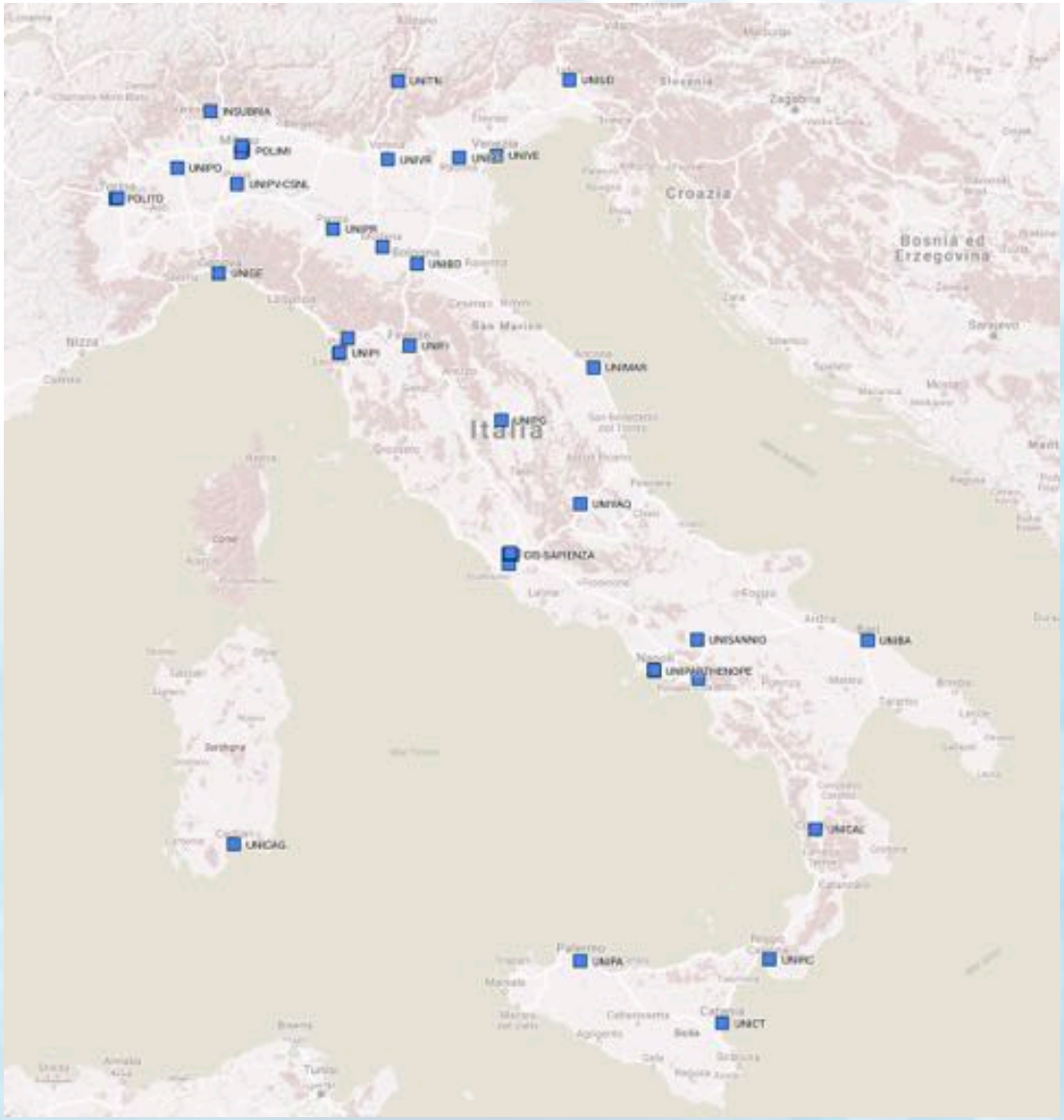
Luca Montanari



Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini
Cybersecurity National Lab

cini Cybersecurity National Lab



CIS Sapienza

Cyber Intelligence and information Security

cini Cybersecurity National Lab

CIS Sapienza

Cyber Intelligence and information Security

CyberChallenge.it

ITASEC17

ITALIAN CONFERENCE ON CYBERSECURITY

Venice, 17-20 January 2017

Università Ca'Foscari Venezia

cini Cybersecurity National Lab

FILIERA SICURA

MASTER OF SCIENCE IN CYBERSECURITY

OBIETTIVI FORMATIVI

La laurea magistrale in Cybersecurity dell'Università di Roma "La Sapienza" è la prima laurea magistrale di questo genere offerta in Italia. Il corso di studio si caratterizza per un'offerta didattica interdisciplinare che raccoglie contributi dell'informatica, dell'ingegneria, della statistica, delle scienze giuridico-economiche e organizzative, insieme a conoscenze specifiche dei principali domini applicativi di protezione contro i cyber-attacchi.

In particolare, la laurea magistrale in Cybersecurity offre le conoscenze professionali, sia dal punto di vista tecnologico sia organizzativo sia normativo, necessarie per definire, supervisionare e coordinare i processi di analisi e governo della sicurezza di sistemi ed informazioni nell'ambito di infrastrutture informatiche complesse, per organizzare la protezione da cyber-attacchi, attuare i processi di gestione degli incidenti informatici, gestire il recupero in caso di attacco avvenuto con successo, sviluppare attraverso metodologie avanzate software sicuro e, infine, per inquadrare gli aspetti legati alla sicurezza di sistemi e informazioni all'interno delle politiche aziendali di gestione del rischio.

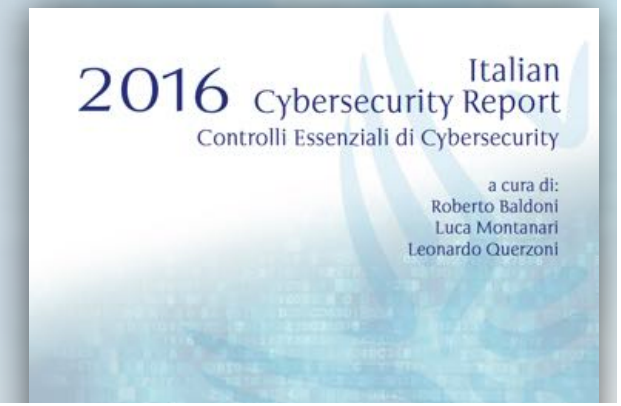
La forte enfasi su una formazione multidisciplinare sia tecnologica, sia giuridica, sia economica caratterizza l'unicità dei contenuti della laurea magistrale in Cybersecurity, prima in Italia ad offrire all'interno di un percorso altamente specializzante, corsi indirizzati all'*ethical hacking*, *analisi di malware*, *digital forensics* e *security governance*.

cini Cybersecurity National Lab

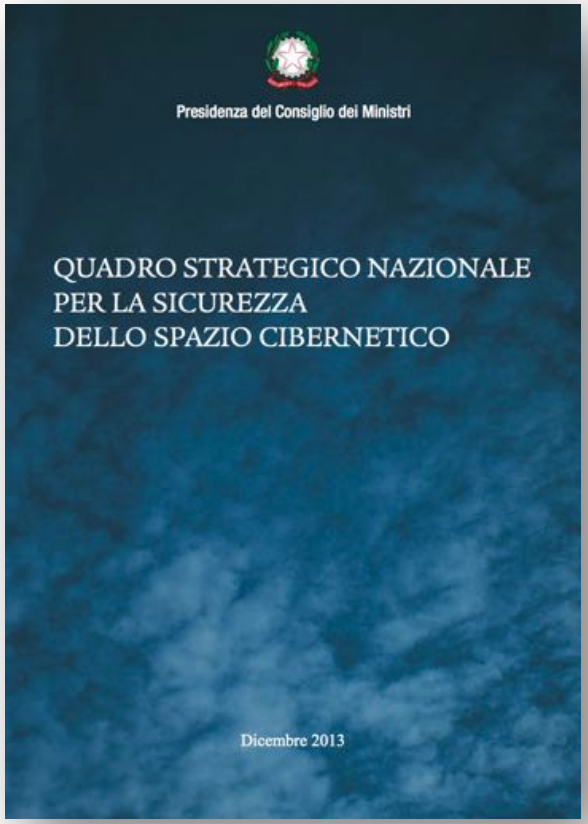
CIS Sapienza

Cyber Intelligence and information Security

- Malware analysis
- Malware detection
- Penetration testing
- Vulnerability assessment
- Dependability
- Stream Processing
- Machine Larning for security
- Big Data analysis
- Big Data for Security
- Framework e Standard
- ...



Nascita del Framework



Dalla Strategia Nazionale al Framework Nazionale

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cybersecurity National Lab

Nascita del Framework

INDIRIZZO OPERATIVO 7

COMPLIANCE A *STANDARD* E PROTOCOLLI DI SICUREZZA

La compliance *a* standard *e protocolli di sicurezza, elaborati sia a livello nazionale che internazionale, consente di garantire un comune ed elevato livello qualitativo nell'assicurare la protezione cibernetica e la sicurezza informatica dei sistemi e delle reti.*

7.2	*Documenti di riferimento*	a. Elaborare e pubblicare documenti di riferimento quali manuali, elenchi di procedure *standard* e raccomandazioni (*best practices* di settore), tassonomia e lessico uniforme da utilizzare per lo scambio di informazioni

Nascita del Framework

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

AON Deloitte. Enel eni hermesbay KPMG INTELLIUM

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

COMPUTER EMERGENCY RESPONSE TEAM PUBBLICA AMMINISTRAZIONE
CERT - PA
Agenzia per l'Italia Digitale

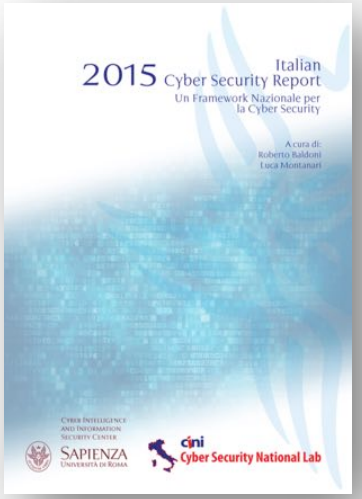
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Ministero dello Sviluppo Economico

CERT nazionale Italia

Microsoft

pwc



2014

- Strategia Nazionale 27/12/2013
- Definizione degli obiettivi
- Definizione del tavolo di lavoro

2015

- Allargamento del tavolo a imprese e PA (PPP)
- 4 Febbraio 2016

CYBER INTELLIGENCE AND INFORMATION SECURITY CENTER
SAPIENZA UNIVERSITÀ DI ROMA

cini Cybersecurity National Lab

Obiettivi iniziali

- Portare la consapevolezza del rischio cyber ai massimi livelli aziendali
  - non più una cosa per soli tecnici
  - portare le organizzazioni a considerare il rischio cyber come rischio economico parte del risk management

- Considerare il panorama economico italiano
  - 69% del PIL prodotto da Piccole-Medie Imprese
  - Pochissime grandi imprese nazionali, 0,1%

Obiettivi iniziali

- Creare qualcosa che sia riconosciuto a livello internazionale
  - migliorare la capacità di information sharing
  - innalzare il livello di duty of care nazionale

- Non reinventare la ruota
  - non ha senso creare un nuovo framework da zero
  - siamo partiti dal **NIST Framework for Improving Critical Infrastructure Cybersecurity**

Il Framework Nazionale è uno strumento di autovalutazione del rischio cyber

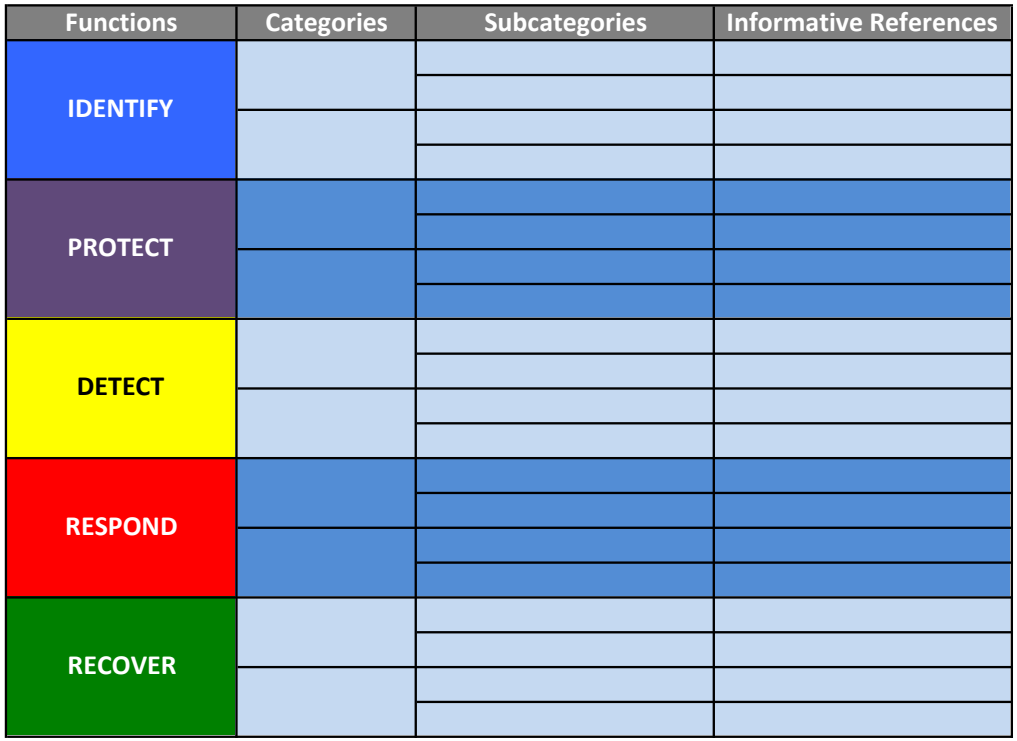
Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cybersecurity National Lab

Il Framework Nazionale è uno strumento di autovalutazione del rischio cyber

- Non è uno standard (non è certificabile)
- Permette di definire il proprio **profilo attuale** e il **profilo target**
- Aiuta nella definizione della **roadmap** per passare dal profilo attuale al profilo target

NIST Framework for Improving Critical Infrastructure Cybersecurity

- Framework core
- Profiles



Framework Nazionale per la Cybersecurity

- Framework core
- Profiles

Abbiamo Aggiunto:

- Livelli Priorità*
- Livelli di Maturità*
- Linee Guida*
- Riferimenti normativi (privacy, CAD, altro*)
- Metodologia di contestualizzazione

*validi per nell'ambito della contestualizzazione

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cybersecurity National Lab

Framework Nazionale per la Cybersecurity

Function	Category	Subcategory	Priorità	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	ALTA	- CCS CSC 1 - COBIT 5 BAI09.01, BAI09.02 - ISA 62443-2-1:2009 4.2.3.4 - ISA 62443-3-3:2013 SR 7.8 - ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 - NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	ALTA	- CCS CSC 2 - COBIT 5 BAI09.01, BAI09.02, BAI09.05 - ISA 62443-2-1:2009 4.2.3.4 - ISA 62443-3-3:2013 SR 7.8 - ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 - NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.	BASSA	- CCS CSC 1 - COBIT 5 DSS05.02 - ISA 62443-2-1:2009 4.2.3.4 - ISO/IEC 27001:2013 A.13.2.1 - NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	NON SELEZIONATA	- COBIT 5 APO02.02 - ISO/IEC 27001:2013 A.11.2.6 - NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	MEDIA	- COBIT 5 APO03.03, APO03.04, BAI09.02 - ISA 62443-2-1:2009 4.2.3.6 - ISO/IEC 27001:2013 A.8.2.1 - NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 - **Obbligatorio per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. a) del CAD**
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	ALTA	- COBIT 5 APO01.02, DSS06.03 - ISA 62443-2-1:2009 4.3.2.3.3 - ISO/IEC 27001:2013 A.6.1.1 - NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Business Environment (ID.BE): La missione dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	ID.BE-1:Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	NON SELEZIONATA	- COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 - ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 - NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	NON SELEZIONATA	- COBIT 5 APO02.06, APO03.01 - NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione.	MEDIA	- COBIT 5 APO02.01, APO02.06, APO03.01 - ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 - NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	MEDIA	- ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 - NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici	MEDIA	- COBIT 5 DSS04.02 - ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 - NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

della contestualizzazione

Contestualizzazioni

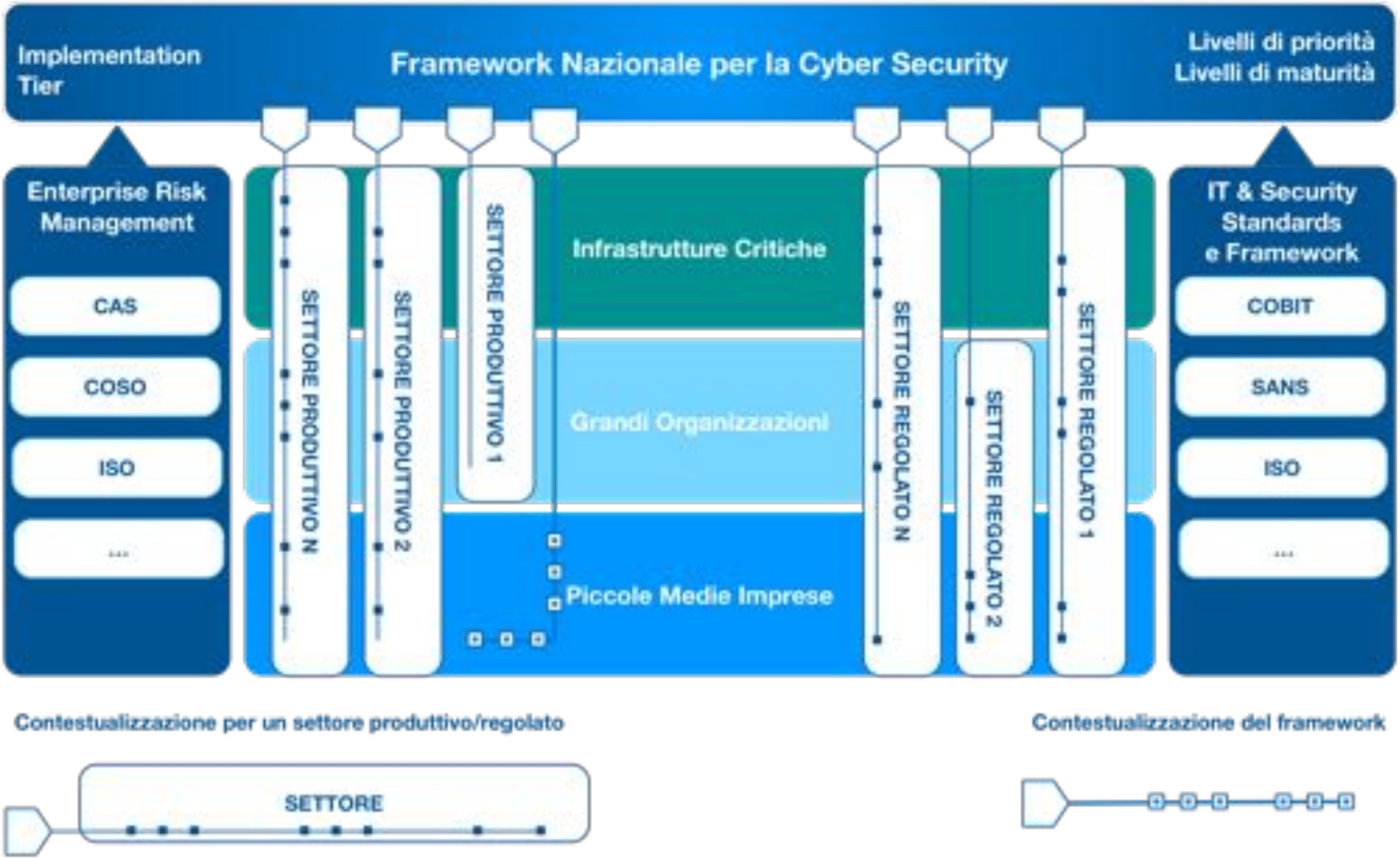
Il Framework può essere "customizzato" tramite:

- la **selezione** delle Subcategory
- **definizione** di livelli di **priorità** per ogni subcategory
- **definizione** livelli di **maturità** per ogni subcategory

Scope della Contestualizzazione

La singola contestualizzazione può essere valida per **organizzazioni**:

- di un dato **settore economico**/produttivo
- di una certa **dimensione**
- appartenenti a un **settore regolato**
  - per pubbliche amministrazioni centrali/locali
  - banche
  - …
- Per business unit di IC o GI



Contestualizzazione per un settore produttivo/regolato

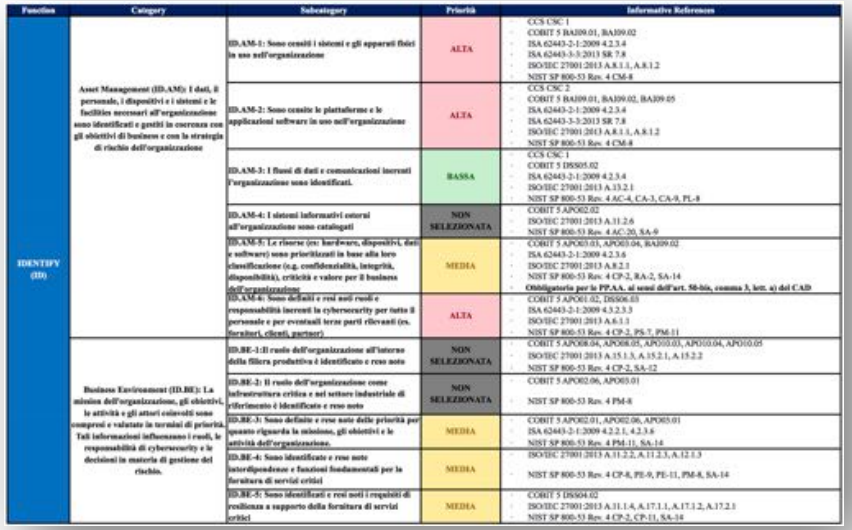
Contestualizzazione del framework

Vantaggi per le grandi imprese

- Strumento per la **top management awareness**
- Un aiuto a definire **piani di spesa** per la gestione del rischio cyber
- Gestione della **catena di approvvigionamento**
- Strumento per rafforzare/rivedere la gestione del **rischio cyber**
- Strumento di **comunicazione** con le altre imprese

Vantaggi per le PMI

- Qualcosa da cui partire*!
- Una contestualizzazione del Framework dedicata a loro
- Guida all'implementazione delle subcategory a priorità alta



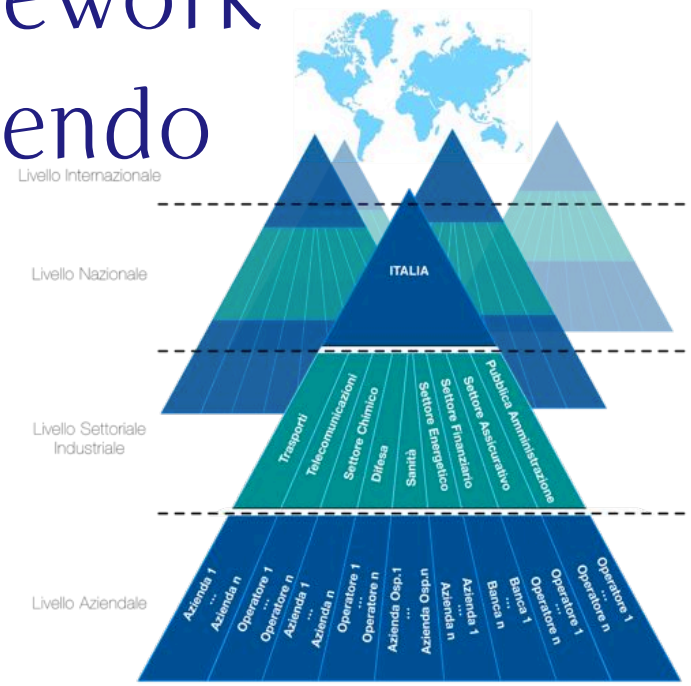
Function	Category	Subcategory	Priorità	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	ALTA	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	ALTA	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: I flussi di dati e comunicazioni interni l'organizzazione sono identificati.	BASSA	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	NON SELEZIONATA	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione.	MEDIA	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · **Obbligatoria per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. a) del CAD**
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	ALTA	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Business Environment (ID.BE): La missione dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	ID.BE-1:Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	NON SELEZIONATA	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	NON SELEZIONATA	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione.	MEDIA	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	MEDIA	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici	MEDIA	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

* non abbastanza...

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cybersecurity National Lab

Vantaggi per la Nazione

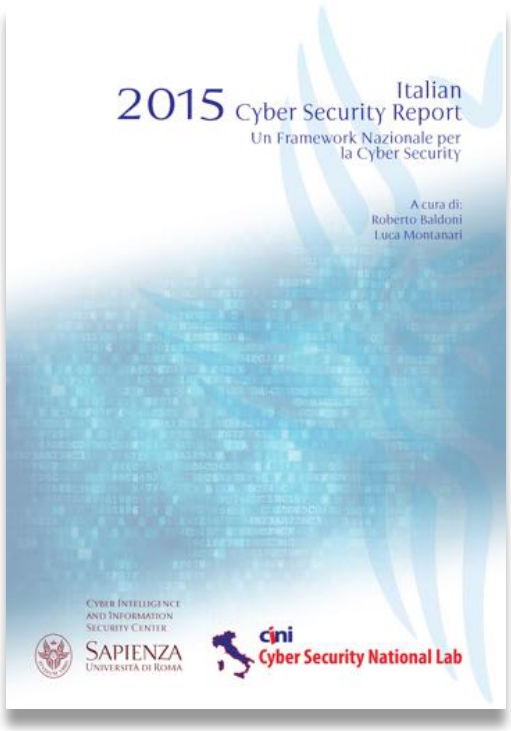
- Fornire un **linguaggio comune** a diversi soggetti in modo da poter emanare regole in maniera coerente e.g.,Garante Privacy, AGID, PCM, ecc.
- **Internazionalità** del framework
- Poter dire che stiamo facendo qualcosa!



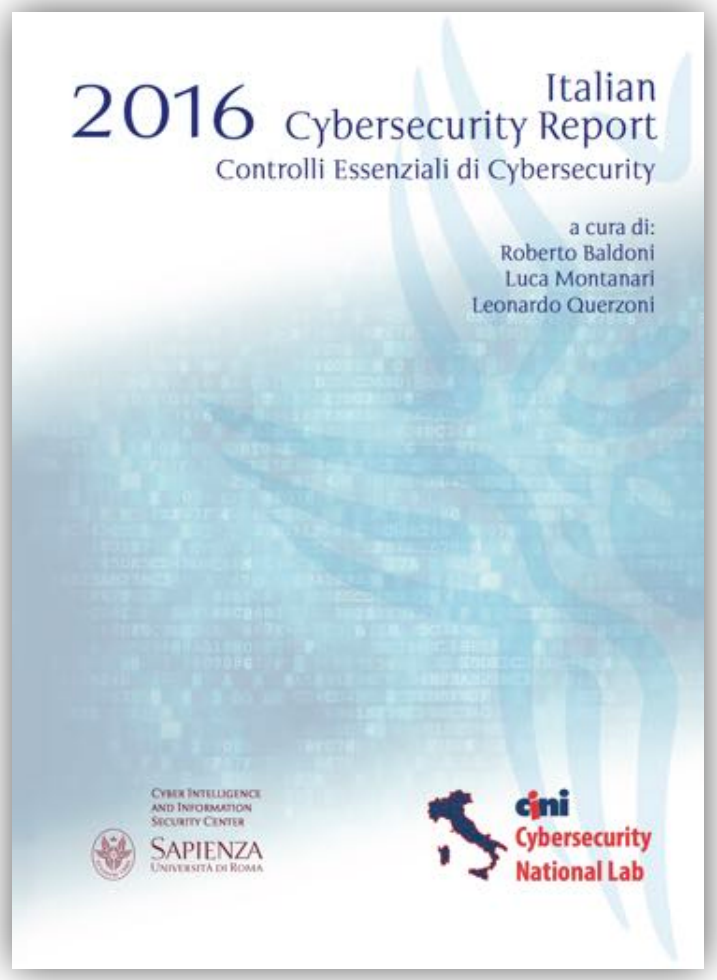
Framework Nazionale

- **Più generale del** NIST CI-Framework
  - le contestualizzazioni permettono di creare Framework "custom"
- Viene mantenuta la **compliance** con il NIST CI-Framework
  - riconosciuto internazionalmente
- **Profili di sicurezza** più accurati
  - sono definiti sui livelli di maturità
- **Riconosciuto a livello nazionale**
  - potrebbe rafforzare la **supply chain** dell'intero panorama nazionale
  - Fornisce un linguaggio comune per le **interazioni tra pubblico e privato**

CONTROLLI ESSENZIALI DI CYBERSECURITY



Controlli Essenziali sono parte dello stesso processo del Framework Nazionale



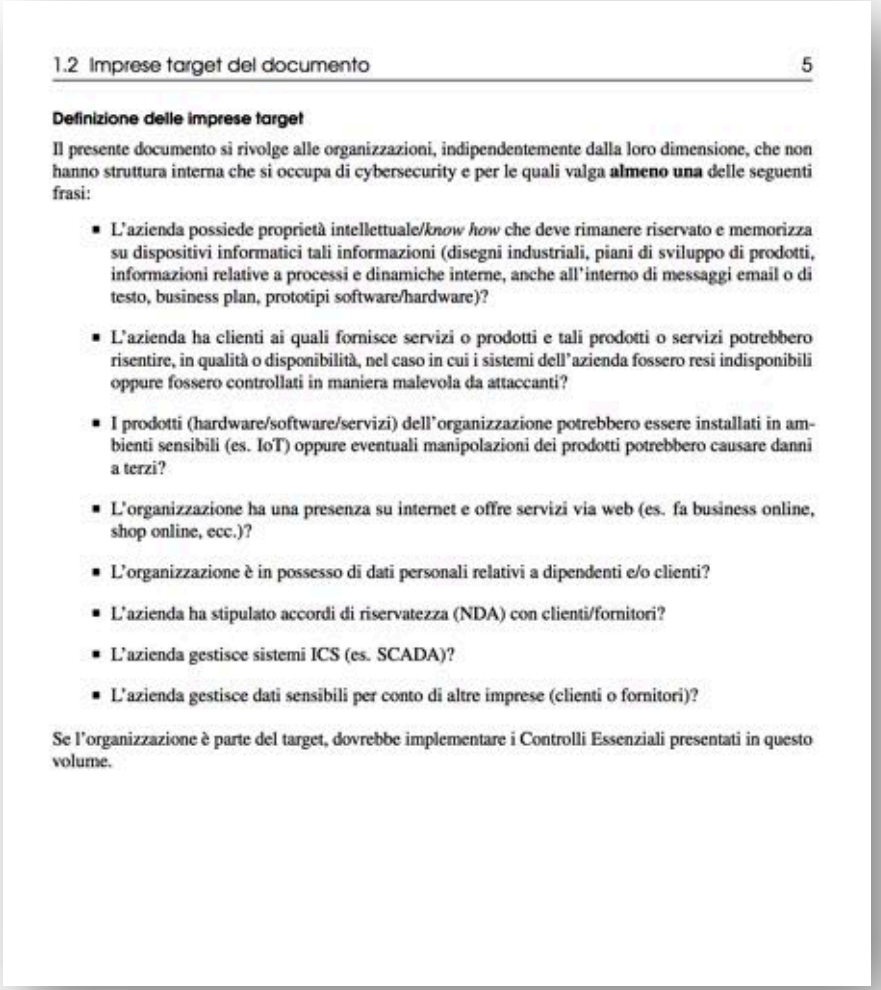
Strumento che permette di "iniziare" a parlare la lingua del Framework Nazionale dedicato a uno specifico target d'imprese

Imprese target

Le imprese che non hanno sufficienti risorse per adottare il Framework Nazionale

Razionale:

- Possibilità di danni verso terzi in servizi/prodotti
- Esposizione su internet
- Dati sensibili, personali, know how nei dispositivi



1.2 Imprese target del documento 5

Definizione delle imprese target

Il presente documento si rivolge alle organizzazioni, indipendentemente dalla loro dimensione, che non hanno struttura interna che si occupa di cybersecurity e per le quali valga **almeno una** delle seguenti frasi:

- L'azienda possiede proprietà intellettuale/*know how* che deve rimanere riservato e memorizza su dispositivi informatici tali informazioni (disegni industriali, piani di sviluppo di prodotti, informazioni relative a processi e dinamiche interne, anche all'interno di messaggi email o di testo, business plan, prototipi software/hardware)?
- L'azienda ha clienti ai quali fornisce servizi o prodotti e tali prodotti o servizi potrebbero risentire, in qualità o disponibilità, nel caso in cui i sistemi dell'azienda fossero resi indisponibili oppure fossero controllati in maniera malevola da attaccanti?
- I prodotti (hardware/software/servizi) dell'organizzazione potrebbero essere installati in ambienti sensibili (es. IoT) oppure eventuali manipolazioni dei prodotti potrebbero causare danni a terzi?
- L'organizzazione ha una presenza su internet e offre servizi via web (es. fa business online, shop online, ecc.)?
- L'organizzazione è in possesso di dati personali relativi a dipendenti e/o clienti?
- L'azienda ha stipulato accordi di riservatezza (NDA) con clienti/fornitori?
- L'azienda gestisce sistemi ICS (es. SCADA)?
- L'azienda gestisce dati sensibili per conto di altre imprese (clienti o fornitori)?

Se l'organizzazione è parte del target, dovrebbe implementare i Controlli Essenziali presentati in questo volume.

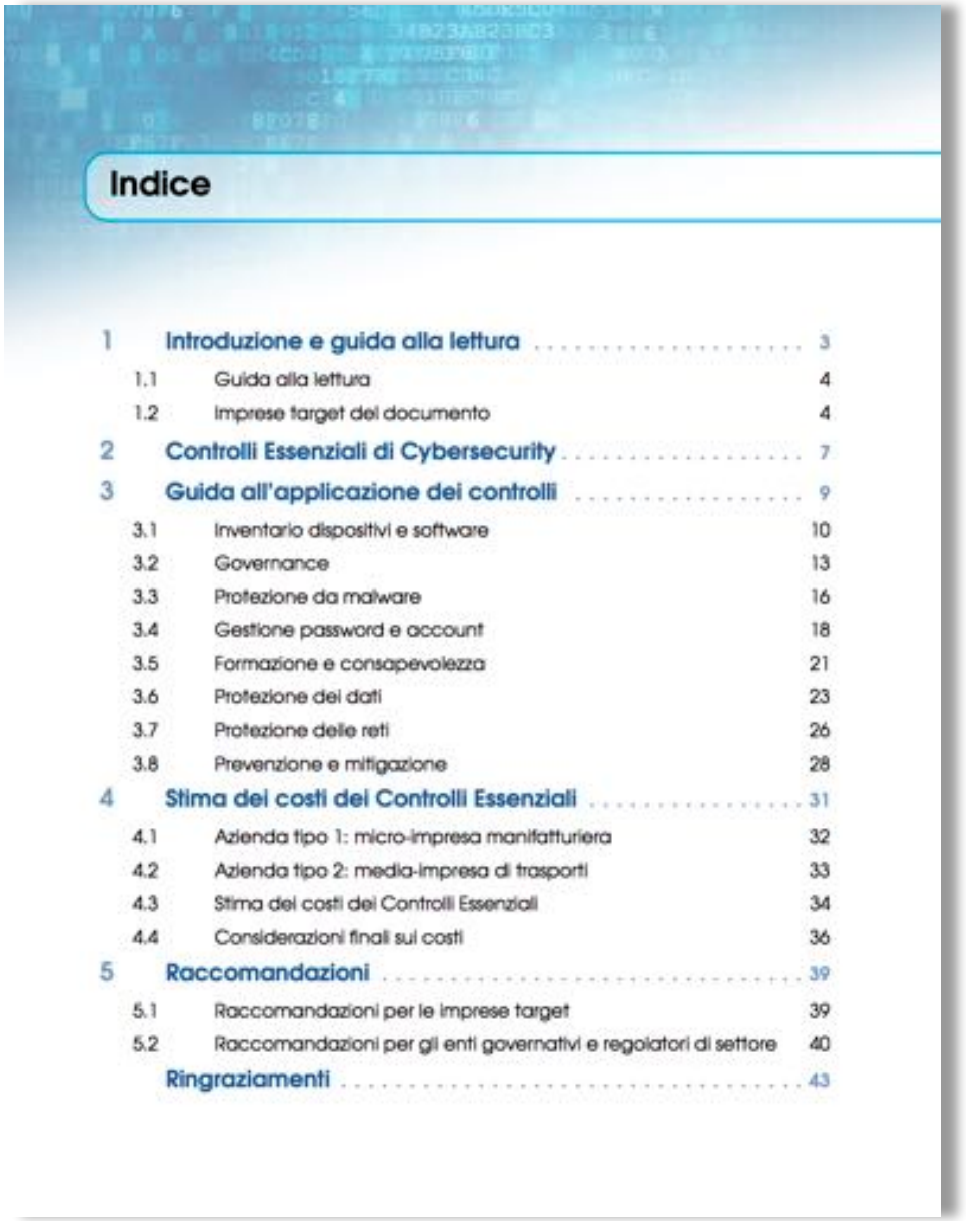
Imprese target

Se l'organizzazione è parte del target dovrebbe implementare tutti i Controlli Essenziali di Cybersecurity

Definizione di controllo essenziale

Pratica di cybersecurity che, se ignorata, causa un aumento inaccettabile del rischio

Il Cybersecurity Report 2016



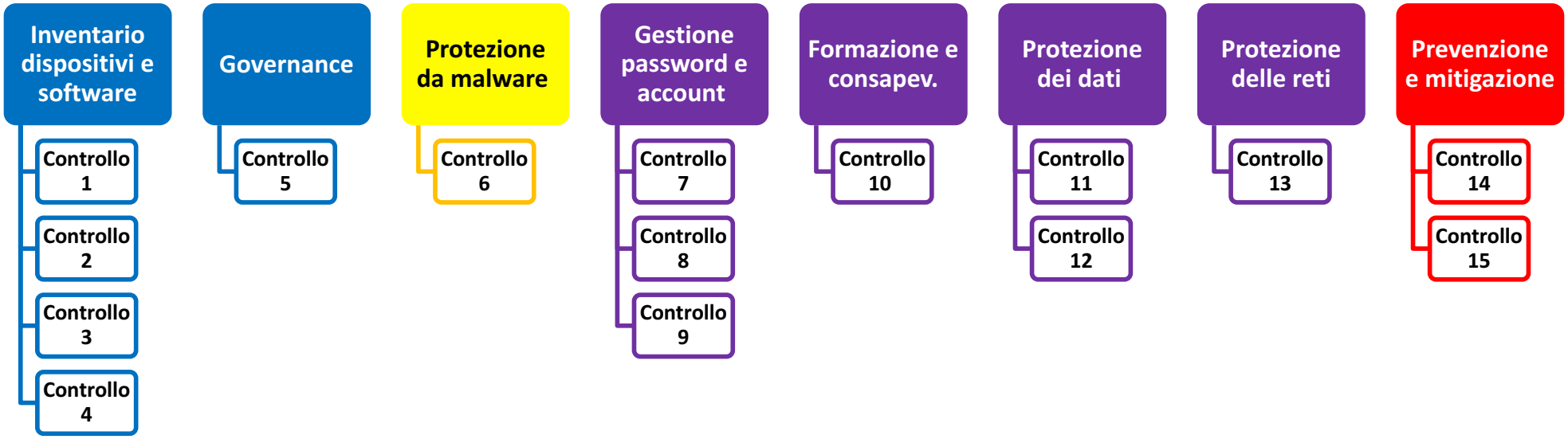
Indice

I 15 Controlli Essenziali di Cybersecurity

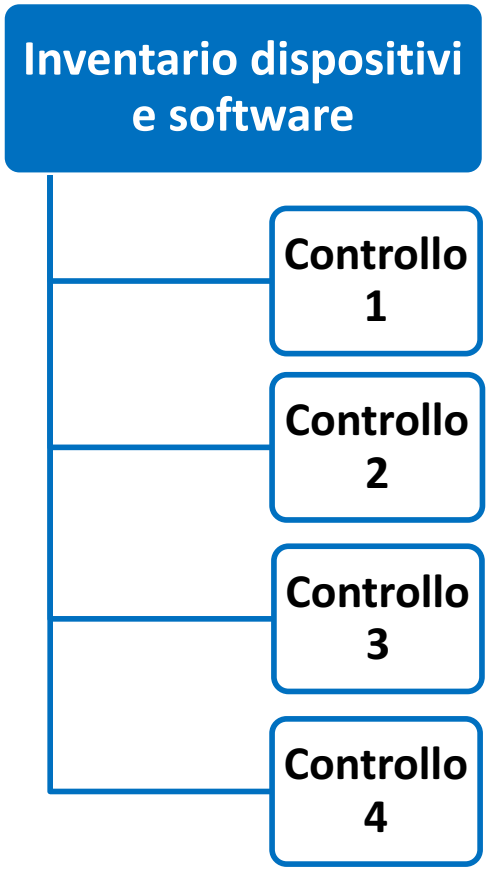
Tabella 2.1: I Controlli Essenziali di Cybersecurity

1	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
2	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc…) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.
3	Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
4	È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
5	Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.
6	Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.
7	Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).
8	Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
9	Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.
10	Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, …). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.
11	La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.
12	Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.
13	Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).
14	In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
15	Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

I 15 Controlli Essenziali di Cybersecurity



I 15 Controlli Essenziali di Cybersecurity



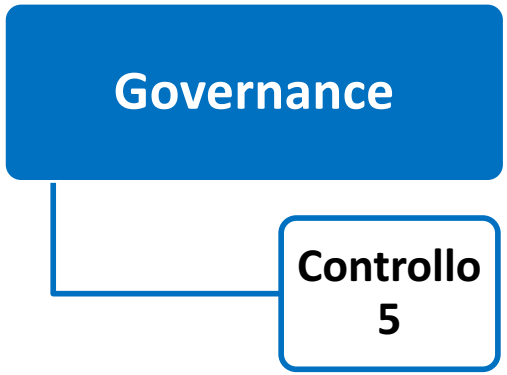
Creare inventari di **sistemi, dispositivi, software, servizi**

Minimizzare l'esposizione sui social/servizi da terzi

Creare inventari di **informazioni, dati e sistemi critici**

Nominare un **referente per la cybersecurity**

I 15 Controlli Essenziali di Cybersecurity



Identificare e **rispettare le leggi** e i regolamenti relativi alla cybersecurity

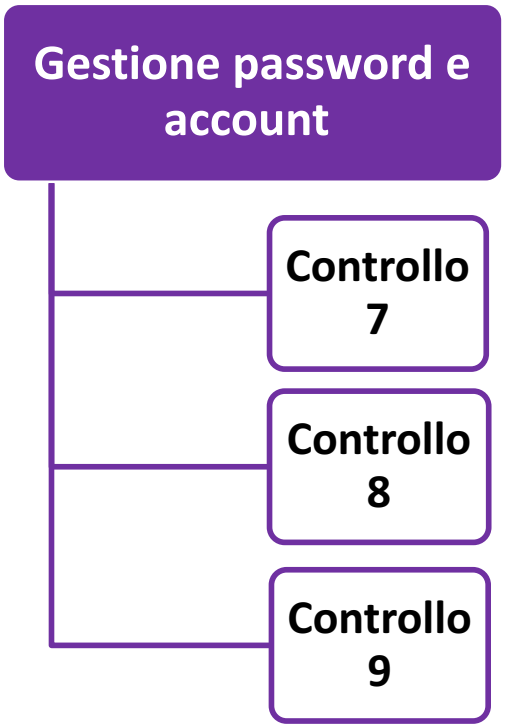
I 15 Controlli Essenziali di Cybersecurity

Protezione da Malware

Controllo 6

Utilizzare e mantenere aggiornato **software antimalware** su tutti i dispositivi che lo consentono

I 15 Controlli Essenziali di Cybersecurity



Utilizzare **password lunghe e diverse per ogni account, dismissione vecchi account, autenticazione forte**

Effettuare l'accesso ai sistemi usando **utenze personali**, non condivise con altri

Applicare il **principio del privilegio minimo** di accesso alle risorse

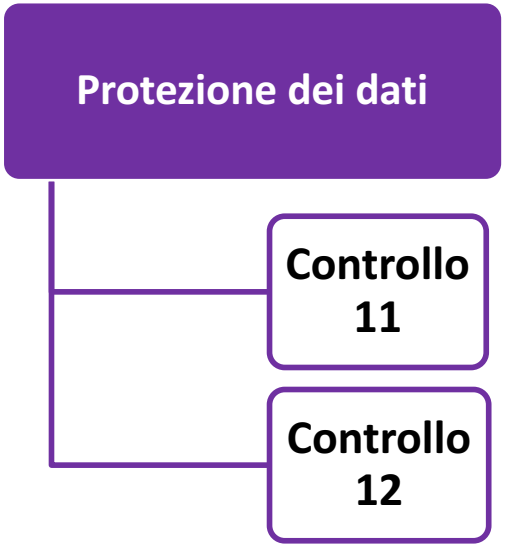
I 15 Controlli Essenziali di Cybersecurity

Formazione e consapevolezza

Controllo 10

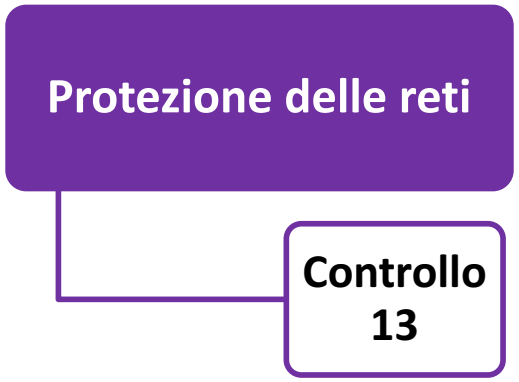
Eseguire adeguata **formazione** per tutto il personale, coordinata dai vertici aziendali

I 15 Controlli Essenziali di Cybersecurity



Effettuare la **configurazione iniziale** dei dispositivi tramite di esperti

Definire procedure di **backup** dei dati critici



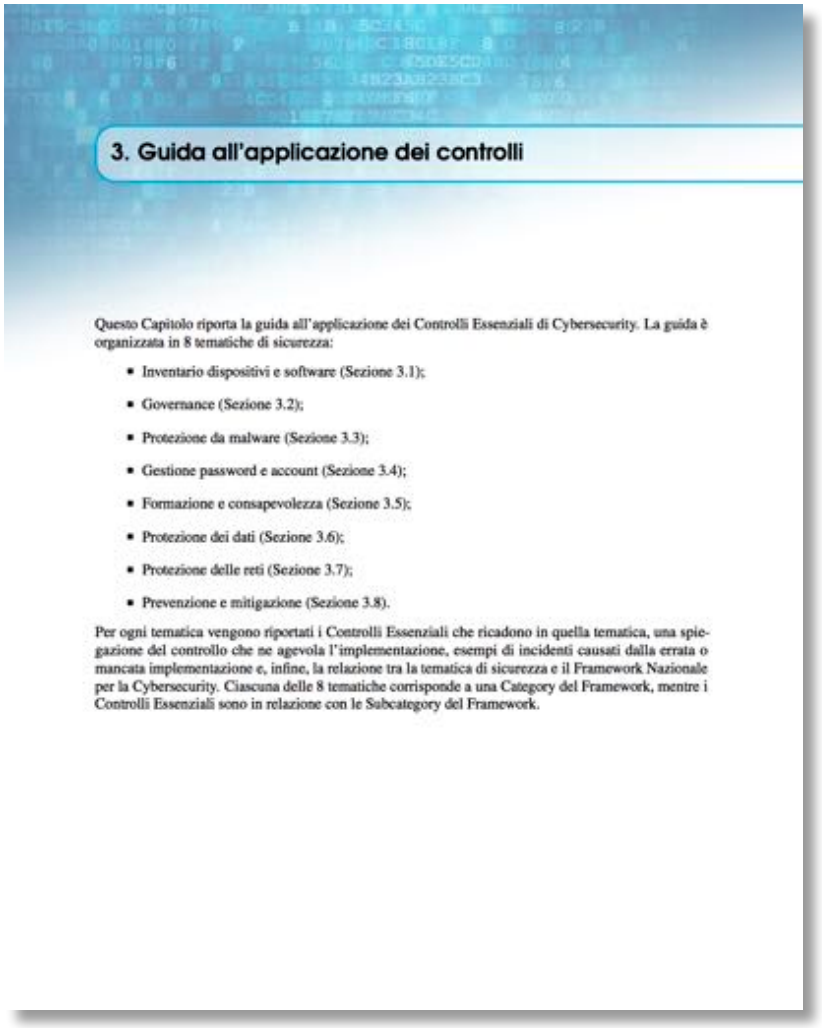
Utilizzare dispositivi di **protezione delle reti**

I 15 Controlli Essenziali di Cybersecurity

In caso di incedente **informare i responsabili**. Il ripristino viene curato da **personale esperto**

Eseguire gli **aggiornamenti software/firmware** e dismettere hardware e software **non più supportato**

Guida all'applicazione



3. Guida all'applicazione dei controlli

Questo Capitolo riporta la guida all'applicazione dei Controlli Essenziali di Cybersecurity. La guida è organizzata in 8 tematiche di sicurezza:

- Inventario dispositivi e software (Sezione 3.1);
- Governance (Sezione 3.2);
- Protezione da malware (Sezione 3.3);
- Gestione password e account (Sezione 3.4);
- Formazione e consapevolezza (Sezione 3.5);
- Protezione dei dati (Sezione 3.6);
- Protezione delle reti (Sezione 3.7);
- Prevenzione e mitigazione (Sezione 3.8).

Per ogni tematica vengono riportati i Controlli Essenziali che ricadono in quella tematica, una spiegazione del controllo che ne agevola l'implementazione, esempi di incidenti causati dalla errata o mancata implementazione e, infine, la relazione tra la tematica di sicurezza e il Framework Nazionale per la Cybersecurity. Ciascuna delle 8 tematiche corrisponde a una Category del Framework, mentre i Controlli Essenziali sono in relazione con le Subcategory del Framework.

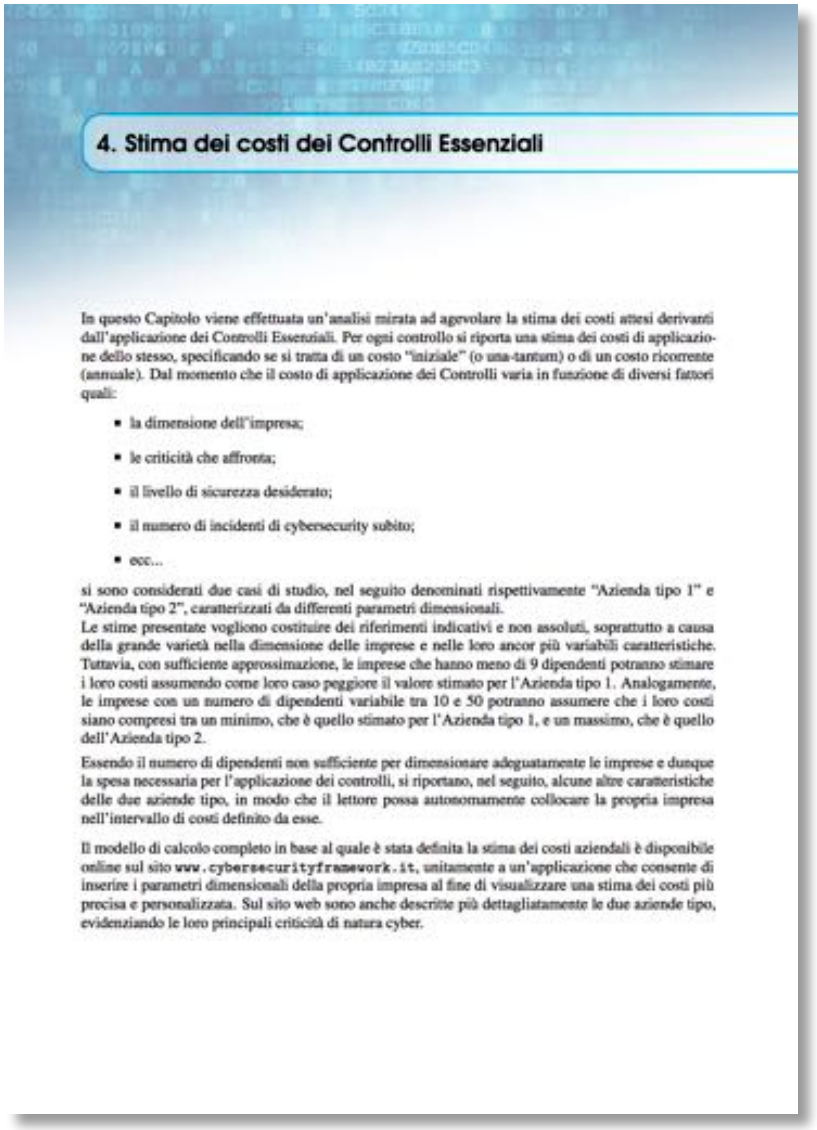
Organizzata per **tematiche di sicurezza, per ognuna:**

- **Descrizione dei Controlli Essenziali**
- **Esempi di incidenti** dovuti alla carente/errata applicazione
- Relazione tra **Controlli Essenziali e Framework Nazionale**

Relazione con il Framework Nazionale

FUNCTION	CATEGORY	SUBCATEGORY	CONTROLLO
PROTECT (PR)	Access Control (PR.AC): L'accesso agli asset ed alle relative risorse è limitato al personale, ai processi, ai dispositivi, alle attività ed alle transazioni effettivamente autorizzate	PR.AC-1:Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate	**7 – Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).**
		PR.AC-3: L'accesso remoto alle risorse è amministrato	**8 – Il personale autorizzato all'accesso, sia esso remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati**
		PR.AC-4: Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	**9 – Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.**

Stima dei costi



4. Stima dei costi dei Controlli Essenziali

In questo Capitolo viene effettuata un'analisi mirata ad agevolare la stima dei costi attesi derivanti dall'applicazione dei Controlli Essenziali. Per ogni controllo si riporta una stima dei costi di applicazione dello stesso, specificando se si tratta di un costo "iniziale" (o una-tantum) o di un costo ricorrente (annuale). Dal momento che il costo di applicazione dei Controlli varia in funzione di diversi fattori quali:

- la dimensione dell'impresa;
- le criticità che affronta;
- il livello di sicurezza desiderato;
- il numero di incidenti di cybersecurity subito;
- ecc...

si sono considerati due casi di studio, nel seguito denominati rispettivamente "Azienda tipo 1" e "Azienda tipo 2", caratterizzati da differenti parametri dimensionali.
Le stime presentate vogliono costituire dei riferimenti indicativi e non assoluti, soprattutto a causa della grande varietà nella dimensione delle imprese e nelle loro ancor più variabili caratteristiche. Tuttavia, con sufficiente approssimazione, le imprese che hanno meno di 9 dipendenti potranno stimare i loro costi assumendo come loro caso peggiore il valore stimato per l'Azienda tipo 1. Analogamente, le imprese con un numero di dipendenti variabile tra 10 e 50 potranno assumere che i loro costi siano compresi tra un minimo, che è quello stimato per l'Azienda tipo 1, e un massimo, che è quello dell'Azienda tipo 2.

Essendo il numero di dipendenti non sufficiente per dimensionare adeguatamente le imprese e dunque la spesa necessaria per l'applicazione dei controlli, si riportano, nel seguito, alcune altre caratteristiche delle due aziende tipo, in modo che il lettore possa autonomamente collocare la propria impresa nell'intervallo di costi definito da esse.

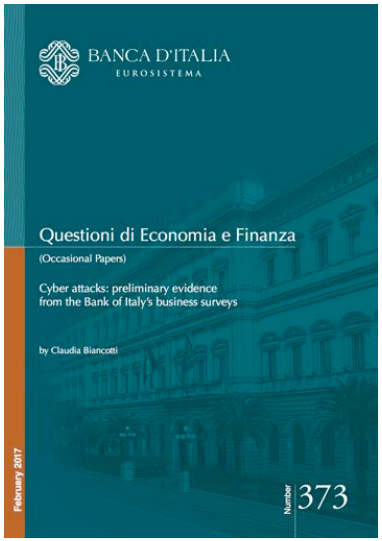
Il modello di calcolo completo in base al quale è stata definita la stima dei costi aziendali è disponibile online sul sito `www.cybersecurityframework.it`, unitamente a un'applicazione che consente di inserire i parametri dimensionali della propria impresa al fine di visualizzare una stima dei costi più precisa e personalizzata. Sul sito web sono anche descritte più dettagliatamente le due aziende tipo, evidenziando le loro principali criticità di natura cyber.

Cerchiamo di **fornire una stima dei costi** di applicazione dei controlli:

- Basata su un modello (disponibile a sul sito)
- Prendendo come riferimento **2 aziende tipo italiane:**
  - Micro da 9 dipendenti
  - Piccola da 50 dipendenti

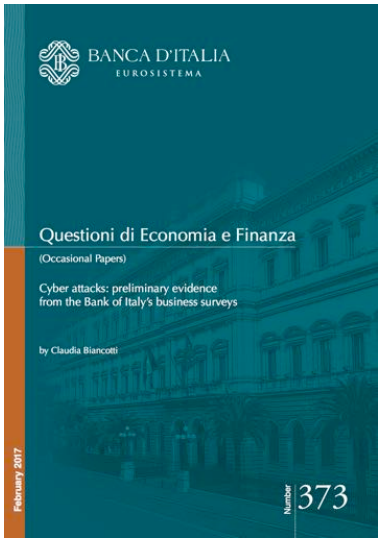
La cybersecurity è ancora un costo certo a fronte di danno incerto?

Stima dei costi



Tra settembre 2015 e settembre 2016 il **45.2%** delle imprese **italiane** ha subito almeno un attacco che ha provocato danni

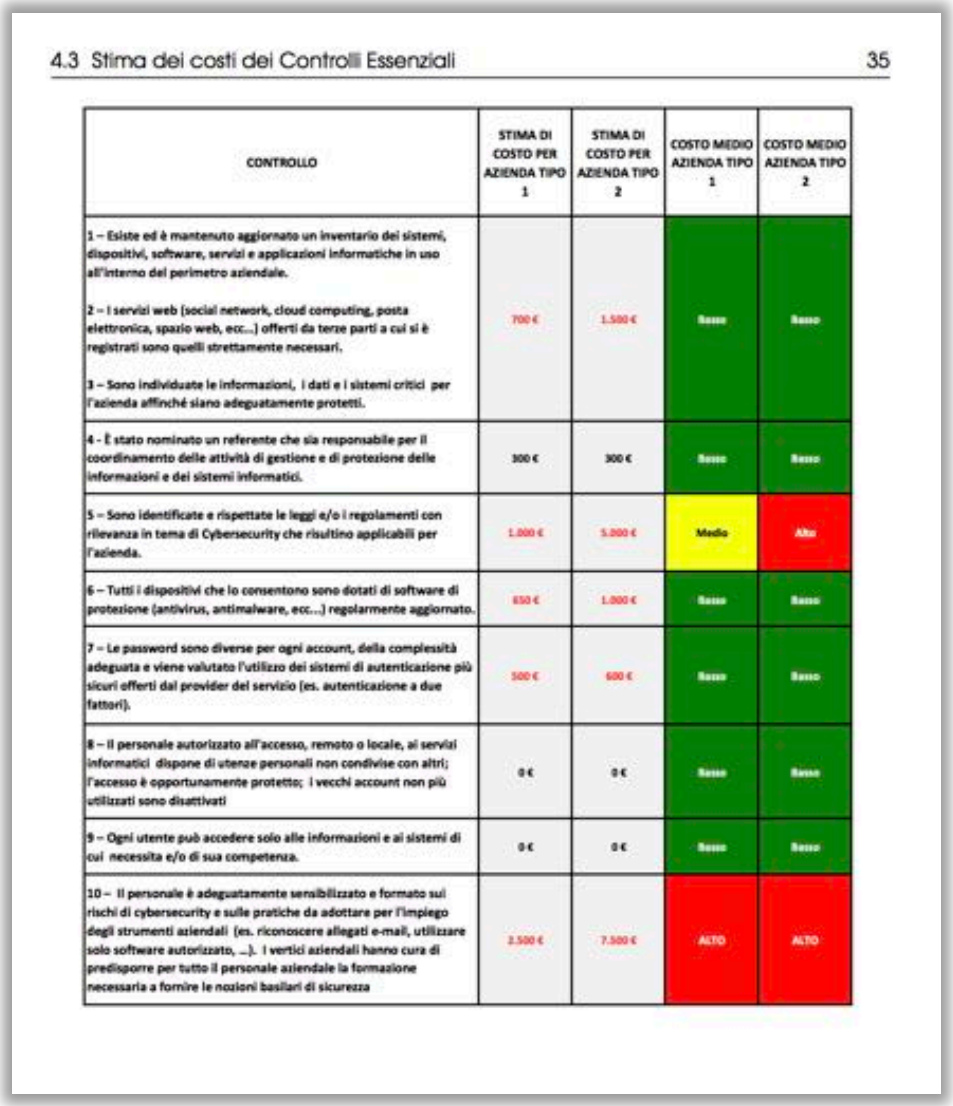
Stima dei costi



Tra settembre 2015 e settembre 2016 il **45.2%** delle imprese **italiane** ha subito almeno un attacco che ha provocato danni

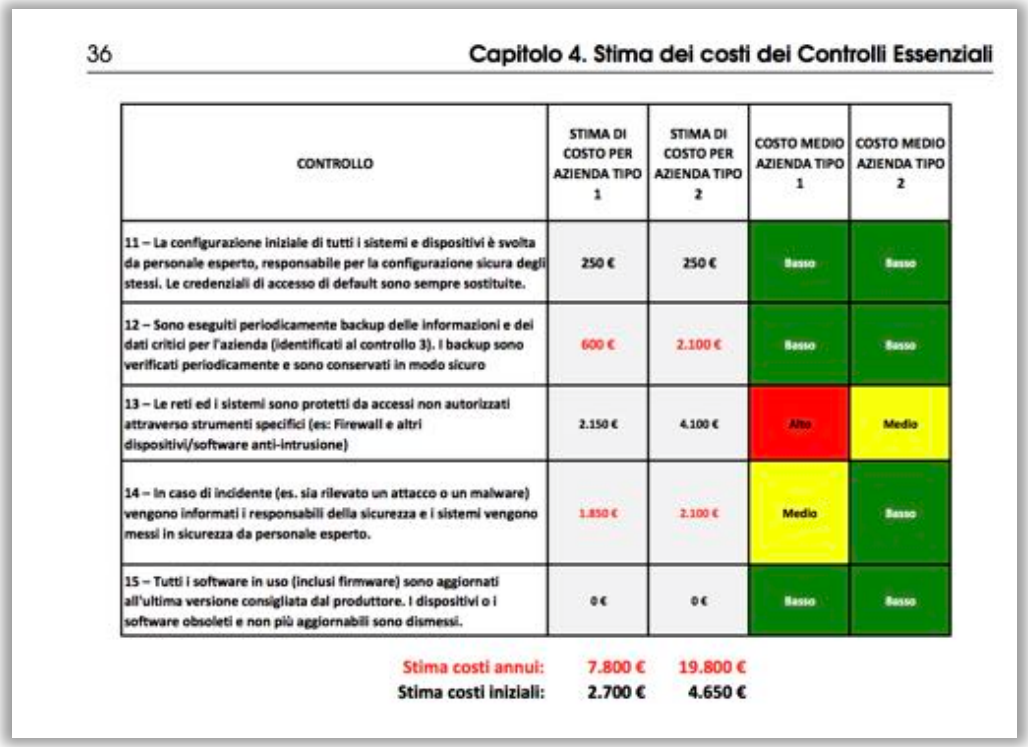
Danno medio per le **PMI** nel mondo **35.000€** per anno

Stima dei costi



4.3 Stima dei costi dei Controlli Essenziali 35

CONTROLLO	STIMA DI COSTO PER AZIENDA TIPO 1	STIMA DI COSTO PER AZIENDA TIPO 2	COSTO MEDIO AZIENDA TIPO 1	COSTO MEDIO AZIENDA TIPO 2
1 – Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale. 2 – I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc...) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. 3 – Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.	700 €	1.500 €	Basso	Basso
4 - È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.	300 €	300 €	Basso	Basso
5 – Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di Cybersecurity che risultino applicabili per l'azienda.	1.000 €	5.000 €	Medio	Alto
6 – Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.	650 €	1.000 €	Basso	Basso
7 – Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).	500 €	600 €	Basso	Basso
8 – Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati	0 €	0 €	Basso	Basso
9 – Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.	0 €	0 €	Basso	Basso
10 – Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, ...). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire le nozioni basilari di sicurezza	2.500 €	7.500 €	ALTO	ALTO



36 Capitolo 4. Stima dei costi dei Controlli Essenziali

CONTROLLO	STIMA DI COSTO PER AZIENDA TIPO 1	STIMA DI COSTO PER AZIENDA TIPO 2	COSTO MEDIO AZIENDA TIPO 1	COSTO MEDIO AZIENDA TIPO 2
11 – La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.	250 €	250 €	Basso	Basso
12 – Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono verificati periodicamente e sono conservati in modo sicuro	600 €	2.100 €	Basso	Basso
13 – Le reti ed i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione)	2.150 €	4.100 €	Alto	Medio
14 – In caso di incidente (es. sia rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.	1.850 €	2.100 €	Medio	Basso
15 – Tutti i software in uso (inclusi firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.	0 €	0 €	Basso	Basso
Stima costi annui:	7.800 €	19.800 €		
Stima costi iniziali:	2.700 €	4.650 €		

In 5 anni
costo cybersecurity dal 41%
al 76% inferiore al danno
medio

Conclusioni

- Il Framework Nazionale è **la lingua comune** della cybersecurity
- I controlli essenziali sono un mezzo per avvicinare le Piccole e Medie imprese al **Framework Nazionale**
- **L'obiettivo per le imprese target è non far più parte del target**

GRAZIE

www.cybersecurityframework.it/csr2016

@CIS_Sapienza
@CyberSecNatLab
@lucamontanari